## REMARKS

Claims 1-20 are currently pending in the subject application and are presently under consideration. Claims 1-4 have been amended as shown on pages 2-4 of the Reply. Claims 17-20 have been newly added to emphasize various novel reporting features of applicants' claimed subject matter.

Applicant's representative thanks Examiner Armouche for considering the points of distinction between the cited reference and the claimed invention conveyed telephonically on October 16, 2008. In particular, distinctions relating to the claimed subject matter's global approach to malware handling versus the cited art's distributed approach were discussed. Moreover, applicants' representative modified the claims herein pursuant to the Examiner's suggestion to recite the novel report feature. It is believed this application is in condition for allowance in view of the comments and amendments made herein.

Favorable reconsideration of the subject patent application is respectfully requested in view of the remarks and amendments herein.

### I. Rejection of Claims 1-4 Under 35 U.S.C. §102(b)

Claims 1-4 stand rejected under 35 U.S.C. §102(b) as being anticipated by White *et al.* ("Anatomy of a Commercial-Grade Immune System", http://citeseer.ist.psu.edu/white99anatomy.html, 1999), hereinafter "White". Withdrawal of this rejection is requested for at least the following reasons. White fails to teach each and every element of independent claims 1-4.

> For a prior art reference to anticipate, 35 U.S.C. §102 requires that "***each and every element*** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) (*quoting Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)) (emphasis added).

Moreover, White fails to disclose each and every limitation of independent claims 1-4.

> A single prior art reference anticipates a patent claim only if it expressly or inherently describes ***each and every limitation*** set forth in the patent claim. *Trintec Industries, Inc. v. Top-U.S.A.*

> *Corp.*, 295 F.3d 1292, 63 USPQ2d 1597 (Fed. Cir. 2002); *See Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the … claim. *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

The claimed subject matter relates to systems and methods for determining whether an executable code module is malware according to the code module's exhibited behavior. A management module or management means receives an executable code module that potentially contains malware. The executable code module is evaluated to determine its type and passed to at least one dynamic behavior evaluation module or means. The code module is executed in a virtual environment where some of its execution behaviors are observed and recorded. The recorded behaviors are compared against known behavior signatures to determine whether a match exists. The results of the comparison are reported based at least in part on the degree of the match. In particular, claim 1 recites *a malware detection system for determining whether a code module is malware according to the code module's exhibited behaviors, the system comprising: at least one dynamic behavior evaluation module, wherein each dynamic behavior evaluation module provides a virtual environment for executing a code module of a particular type, and wherein each dynamic behavior evaluation module records some execution behaviors of the code module as it is executed, wherein the execution behaviors of the code module are recorded into a behavior signature corresponding to the code module; a management module, wherein the management module obtains the code module, and wherein the* ***management module evaluates the code module to determine the code module's type****, and wherein the management module selects a dynamic behavior evaluation module to execute the code module according to the code module's type; a malware behavior signature store storing at least one known malware behavior signature of a known malware; a behavior signature comparison module that obtains the behavior signature of the code module and compares the behavior signature of the code module to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited execution behaviors of the code module match the exhibited behaviors of a known malware; and wherein* ***the malware detection system is configured to report whether the code module is malware based at least in part on the degree that the code module's exhibited execution behaviors match the exhibited behaviors of a***

***known malware***.

White relates to a scalable system and network architecture capable of detecting and curing newly detected malware during periods of peak load. Customer machines submit samples of code that potentially contain a virus to a series of network nodes arranged in a hierarchical fashion. Each node receiving a sample compares the checksum of the sample against the checksums of known viruses. The node determines whether the sample can be handled locally or whether further analysis is needed by a higher up node. Ultimately, if a sample cannot be handled by any network node, the sample is sent to a scalable Virus Analysis Center. All activity inside the Virus Analysis Center is coordinated by a Workflow Supervisor. The Workflow Supervisor parcels out various virus analysis tasks to workload machines as they become available. Moreover, the Workflow Supervisor architecturally isolates these tasks in order to provide an architecture that is robust enough to run continuously.

In the subject Office Action, White is cited as teaching the management module as claimed. Applicants' representative respectfully avers to the contrary. White discloses a distributed system and hierarchical network architecture that is capable of being scaled up during periods of peak virus activity. During such periods, code samples that are unable to be handled locally by network nodes are sent to the Virus Analysis Center. The Workflow Supervisor in the Virus Analysis Center receives the samples and oversees their flow through the various stages of analysis. Notably, in order to determine the type of virus, the Workflow Supervisor sends the sample to a separate workload machine to perform a classification task. After classification, the sample is sent back to the Workflow Supervisor. One or more separate workload machines are then selected to execute the sample and perform further processing. Put another way, the Workflow Supervisor disclosed in White does not participate in virus analysis tasks. By design, the Workflow Supervisor architecturally isolates all analysis tasks in order to provide scalability and robustness. This purpose is further advanced by the distributed nature of the Virus Analysis Center. Conversely, unlike the Workflow Supervisor taught in White, the management module of present invention performs a portion of the malware analysis tasks. In particular, the management module of the present invention obtains the code module, evaluates the code module to determine the code module's type and selects a dynamic behavior evaluation module to execute the code module according to the code module's type.

Furthermore, the claimed invention is configured to report whether the code module is

malware based at least in part on the degree that the code module's exhibited execution behaviors match the exhibited behaviors of a known malware. Conversely, the system and architecture taught in White is not capable of reporting the degree that the code module's exhibited execution behaviors match the exhibited behaviors of a known malware.

In light of the aforementioned comments and amendments, White fails to teach each and every element and limitation recited in independent claim 1, and, therefore, does not anticipate the subject claim. Accordingly, it is respectfully requested that the rejection of independent claim 1 (and claims 5-7 that depend therefrom) under 35 U.S.C. 102(b) be withdrawn.

Likewise, White fails to teach each and every element and limitation recited in independent claim 2. Claim 2 recites *a malware detection system for determining whether a code module is malware according to the code module's exhibited behaviors . . .* ***a management means for*** *obtaining the code module and* ***determining the code module's type*** *for the purpose of selecting a behavior evaluation means to execute the code module according to the code module's type . . . wherein* ***the malware detection system is configured to report whether the code module is malware based at least in part on the degree that the code module's exhibited execution behaviors match the exhibited behaviors of a known malware***. Therefore, for similar reasons as those already discussed regarding independent claim 1, White fails to teach each and every feature recited in independent claim 2. Accordingly, it is respectfully requested that the rejection of independent claim 2 (and claims 8-10 that depend therefrom) under 35 U.S.C. 102(b) be withdrawn.

Additionally, White fails to teach each and every feature recited in independent claim 3. In particular, claim 3 recites . . . ***selecting a dynamic behavior evaluation module according to the executable type of the code module as determined by a management*** *module . . . and* ***reporting whether the code module is malware based at least in part on the degree that the code module's exhibited execution behaviors match the exhibited behaviors of a known malware***. Under a similar reasoning to that discussed regarding independent claim 1, White fails to teach each and every element and limitation recited in independent claim 3. Therefore, it is respectfully requested that the rejection of independent claim 3 (and claims 11-13 that depend therefrom) under 35 U.S.C. 102(b) be withdrawn.

Further, White fails to teach each and every limitation recited in independent claim 4. Claim 4 recites . . . *selecting a dynamic behavior evaluation module according to the executable*

*type of the code module* ***as determined by a management module*** *. . . and* ***reporting whether the code module is malware based at least in part on the degree that the code module's exhibited execution behaviors match the exhibited behaviors of a known malware***. In light of the foregoing reasons, White fails to teach each and every element and limitation recited in independent claim 4. Accordingly, it is respectfully requested that the rejection of independent claim 4 (and claims 14-16 that depend therefrom) under 35 U.S.C. 102(b) be withdrawn.

## CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP2452US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicant's undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Christopher Singh/
Christopher Singh
Reg. No. 61,236

AMIN, TUROCY & CALVIN, LLP
127 Public Square
57TH Floor, Key Tower
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731